A Discussion on the Properties of Physically Unclonable Functions*

Roel Maes, Ingrid Verbauwhede

K.U.Leuven ESAT/COSIC and IBBT
{roel.maes, ingrid.verbauwhede}@esat.kuleuven.be

Abstract. The increasing interest in physically unclonable functions or PUFs and in PUF-based security applications desires a concrete and as formal as possible description of what a PUF is and which properties can be naturally expected. However, the wide and growing variety of different PUF and PUF-like proposals makes such a formalization attempt a non-trivial task. In this work we provide a starting point by developing a concrete, though still informal, description of the minimal requirements a construction needs to meet in order to be called a PUF. Additionally, this study gives an insight into attainable and/or desirable PUF properties and reveals some interesting research directions for future investigation.
Key words: Physically Unclonable Functions, Intrinsic PUFs.

1 Introduction

The formal introduction of the PUF concept, first as physical one-way functions [1], physical random functions [2] and eventually as physical(ly) unclonable functions was done in the beginning of the twenty first century, although some similar and equivalent ideas were introduced much earlier [3,4,5]. Following this introduction, an increasing number of new types of PUFs were proposed, with a tendency towards more integrated constructions. The practical relevance of PUFs for security applications was recognized from the start, with a special focus on the promising properties of physical unclonability and tamper evidence. Over the last couple of years, the interest in PUFs has risen substantially, making them a hot topic in the field of hardware security and leading to an expansion of published results.

There exists a widely accepted notion of which constructions we classify as PUFs (or PUF-like) and which not, but coming up with an appropriate and correct formal translation turns out to be harder as expected. A number of earlier PUF-defining attempts fail to completely capture this notion, either by only restricting themselves to a subclass of PUFs through the introduction of too stringent assumptions, or by not being strict enough and allowing clearly non-PUF constructions. On the other hand, in order to develop PUF-based applications, a correct formalization is highly desirable as a basis for demonstrating

* This overview paper was presented as a talk at the TRUST-2010 Workshop on Security Hardware in Berlin, Germany.

strong security notions. Especially for the recently introduced topic of hardware entangled cryptography [6], a formal PUF model seems inevitable.

In this work, we make a start at defining what we understand to be a PUF. We don't yet provide a highly formal description and we certainly do not claim to have found the one-and-only correct PUF definition, but in stead we identify a number of properties which recur in different works on PUFs. By checking these properties for a representative set of PUF proposals and a number of non-PUF reference cases, we propose a least common subset of properties which distinguish PUFs from other primitives. The best way to get a *feeling* of the accepted notion what a PUF is, we give a brief overview of many different PUF proposals in Sect. 2. Recurring PUF properties are described and checked in Sect. 3 and the PUF-defining properties are identified. In Sect. 4, the main results from this property comparison are discussed and evaluated and a number of critical remarks are made. Finally, we conclude in Sect. 5.

2 Physically Unclonable Functions

2.1 PUF Basics

We start by describing a PUF as a *physical challenge-response procedure*. Note that there are already a number of subtleties in this description, i.e. a PUF is not a purely abstract mathematical concept but is (embedded in) a physical entity, and a PUF is a procedure with some input-output functionality although not necessarily a function in the strict mathematical sense. The inputs to a PUF are generally called *challenges* and we denote them as $x \in \mathcal{X}$ and the outputs are called *responses*, $y \in \mathcal{Y}$. An applied challenge and its measured response are generally called a *challenge-response pair or CRP* (x, y) and a particular PUF is completely described by the relation it enforces between challenges and responses and is referred to as its *CRP behavior*, $\Pi : \mathcal{X} \rightarrow \mathcal{Y} : \Pi(x) = y$.

The fundamental application of PUFs comes from their identification ability. To that end, the concept of inter- versus intra-(class) distances was inherited from the theory about classification and identification. For a set of instantiations of a particular PUF construction, inter- and intra-distances are calculated as follows:

- The desired properties of uniqueness and unclonability should result in substantially different responses to the same challenge for a pair of distinct PUF instances. For a particular challenge, the *inter-distance* between two PUFs is the distance between the two responses resulting from applying this challenge once to both PUFs.
- Noise, measurement uncertainty and external influence often undesirably but inevitably affect the exact value of a PUF's response. For a particular challenge, the *intra-distance* between two evaluations on one single PUF instantiation is the distance between the two responses resulting from applying this challenge twice to one PUF.

We stress that both inter- and intra-distance are measured on a pair of responses resulting from *the same challenge*. For a particular type of PUF, the inter- and intra-distance characteristics are often summarized by providing histograms showing the occurrence of both distances, observed over a number of different challenges and a number of different pairs PUFs. A much-used indicator for both measures are their average values over many PUF pairs and many applied challenges, μ_{inter} for inter-distance and μ_{intra} for intra-distance. Desirable PUF behavior is an as small as possible μ_{intra}, with μ_{inter} as close as possible to 50%, e.g. in case of bit vector responses we would like the responses to the same challenge on different PUFs to differ on average for half of the bits.

2.2 PUF and PUF-like Implementations

Over the last couple of years, an increasing number of different PUF or PUF-like constructions have been proposed. We discuss a number of them in more detail and provide many references to similar proposals.

Optical PUFs were originally introduces as physical one-way functions in [1], which is the first attempt to formally describe the PUF concept in cryptographical terms, i.c. as a physical variant of one-way functions. The core component of an optical PUF is a small transparent token randomly doped with optical scattering particles. When radiated with a laser a complex image with bright and dark spots arises, a so-called speckle pattern. A Gabor filter turns out to be a good feature extractor for such a pattern and the filter output is the response of the optical PUF, while the physical parameters of the laser (location, orientation, wave length,...) are considered the challenge. Due to the complex nature of the interaction of the laser light with the scattering particles, the responses are highly random and unique. The high dependence of the response on the exact (sub-)microscopic physical details of the optical token causes two equally produced tokens to show a radically different CRP behavior and moreover prevents a particular token from being cloned with high precision. Additionally, it was demonstrated that a small physical change to the token, e.g. drilling a microscopic hole, changes the CRP behavior substantially, i.e. the tokens show some form of tamper evidence to invasive attacks. A similar approach towards constructing unclonable optical tokens, based on reflective instead of transparent media, was proposed much earlier in [4].

Coating PUFs [7] attempt to integrate the PUF functionality on an integrated circuit (IC). A special coating is sprayed on top of an IC, containing small and random dielectric particles. Capacitive sensors in the top metal layer of the IC measure the random capacitances caused by the dielectric. As with the optical PUF, the CRP behavior of a coating PUF is highly dependent on the randomized sub-micron details of the coating and is hence to a large extent unique and unclonable. Tamper evidence was also experimentally verified and since the coating resides in the top layer of the IC, this property can be used to make the whole IC tamper evident. PUF(-like) proposals based on similar or slightly different concepts were described in [8] as LC-PUFs and in [9] as RF-DNA.

Intrinsic PUFs are in fact a class of PUF proposals with two additional construction requirements. Firstly, the complete PUF including the measurement equipment should be fully integrated in the embedding device using the PUF, and secondly, this integration can be completely performed using the standard manufacturing flow of the device, i.e. without the need for PUF-specific processing steps or components. It is clear that intrinsic PUFs possibly offer higher security conditions whilst being more cost-effective to implement. A number of intrinsic PUF constructions, all based on digital integrated circuits, have been proposed. The key operation principle for all of them is that they use the inevitable random manufacturing variability between equally produced ICs. This use of the *intrinsic* randomness in the devices avoids a possibly costly explicit introduction of randomness.

A first type of intrinsic PUFs on digital ICs are based on the variability in the delay of a digital signal. *Arbiter PUFs* [10] implement two symmetrical digital delay paths on an IC. A challenge controls the exact delay setting of the lines, and a race condition is introduced by feeding a pulse simultaneously on both. A so-called *arbiter circuit* determines which of both paths was the fastest and outputs a bit accordingly. *Ring oscillator PUFs* [2] are also based on digital delays, but transform them into oscillators by using negative feedback. By measuring the oscillations, a measure for the delay is obtained. Both constructions were implemented and tested on integrated circuits and show a nice PUF behavior. However, it was immediately recognized that due to the specific linear construction of the delay circuit, both PUFs are susceptible to *model-building attacks*, i.e. after observing a relatively small number of CRPs from a PUF, the remaining unseen CRPs can be predicted with high accuracy by modeling the delay paths. To overcome this problem, a number of non-linear variants for arbiter PUFs were proposed [10,11,12], but improved modeling techniques [13] have shown that these constructions are also not immune to prediction. For ring oscillator PUFs, a proposed construction based on differential measurements [11] is apparently secure against model-building, but this comes at a large implementation overhead compared to the original construction.

Another type of digital intrinsic PUFs use the effect of manufacturing variability on the settling state of some memory cell constructions. There are a number of ways for constructing digital memories and a much-used method is using cross-coupled gates. By cross-coupling two gates, e.g. two inverters, a logical *cell* is constructed which can assume two distinct but logically stable states, and by residing in one of both the cell can effectively store one binary digit. This is typically the case for SRAM memories (two cross-coupled inverters), latches (two cross-coupled NAND or NOR gates) and flip-flops. If a logically unstable state is introduced in such a cell, it is not clear to which of both stable states it will converge. As it turns out, the tendency of a particular cell towards one or the other stable state is determined by the slight random subtleties caused by manufacturing variability. This settling state is hence random and unique for a particular device and can be used as a PUF response. SRAM PUFs [14,15] and flip-flop PUFs [16] are constructed by observing the settling state of an SRAM

cell or a flip-flop after the implicit instability caused by a power-up of the device. Latch PUFs [17] and butterfly PUFs [18] observe the stabilizing state after a cell has explicitly been destabilized. In all cases, the challenge to the PUF is the address of a particular cell, with the cell's stabilizing state acting as the response.

Other proposals. For completeness, we provide a very brief overview of other concrete PUF(-like) constructions known to us. A number of proposals for identifying documents and packagings based on measurements of the random arrangement of (paper) fibers were proposed over time [3,5,19,20]. In [21], it was observed that manufacturing variability also affects the precise length of lands and pits on a compact disc and that this can be used to extract a CD fingerprint. So-called magnetic PUFs [22] use the inherent uniqueness of particle patterns in magnetic media and can be used as a unique identifier for magnetic swipe cards. Identification of acoustical delay lines based on instance specific details caused by manufacturing variability was studied in [23]. Two PUFs based on analog measurements of electrical parameters on an IC were proposed in [24] (threshold voltages) and in [25] (resistances).

3 Properties of PUFs

3.1 Property Description

We begin by listing eight regularly occurring properties identified from multiple attempted PUF definitions and give a concise but accurate description of what we mean by them, in order to avoid ambiguity in this and future works. We immediately note that these are not completely formal properties, but a hint towards a more formal description is given. In fact, the informal parts of the property descriptions are clearly marked in sans-serif font.

1. *Evaluatable:* given Π and x, it is easy to evaluate $y = \Pi(x)$. Easy can mean different things. From a theoretical point of view it can mean in polynomial time and resources, while in practice it can mean at a very low cost overhead.
2. *Unique:* $\Pi(x)$ contains some information about the identity of the physical entity embedding Π. This means that, in theory, a set of CRPs from a particular PUF suffices to uniquely identify that PUF in a given population.
3. *Reproducible:* $y = \Pi(x)$ is reproducible up to a small error. The error needs to be small in the considered distance metric. This property distinguishes PUFs from true random number generators (TRNGs).
4. *Physically unclonable:* given Π, it is hard to construct a physical entity containing another PUF $\Pi_\Gamma \neq \Pi$ such that $\forall x \in \mathcal{X} : \Pi_\Gamma(x) \approx \Pi(x)$ up to a small error. The hardness of producing a physical clone even holds for the manufacturer of the original PUF Π and is for that reason also called *manufacturer resistance*. Note that physical unclonability implies uniqueness.
5. *Mathematically unclonable:* given Π, it is hard to construct an (abstract) mathematical procedure f_Γ such that $\forall x \in \mathcal{X} : f_{\Gamma(x)} \approx \Pi(x)$ up to a small error.

6. *Unpredictable:* given only a set $\mathcal{Q} = \{(x_i, y_i = \Pi(x_i))\}, i = 1 \ldots q$, it is hard to predict $\Pi(x_c)$ up to a small error with x_c a random challenge such that $(x_c, \cdot) \notin \mathcal{Q}$. Note that unpredictability is a relaxed form of mathematical unclonability, i.e. mathematical unclonability implies unpredictability.
7. *One-way:* given only y and Π, it is hard to find $x \in \mathcal{X}$ such that $\Pi(x) = y$.
8. *Tamper evident:* altering the physical entity embedding Π transforms $\Pi \rightarrow \Pi'$ such that with high probability $\exists x \in \mathcal{X} : \Pi(x) \neq \Pi'(x)$, not even up to a small error. This means that an invasive tampering attack on the PUF leaves indelible traces in the CRP behavior.

Note that we explicitly distinguish between physical and mathematical unclonability since a construction can be easy to clone physically but not mathematically or vice versa. In order to be truly unclonable, Π needs to be both physically and mathematically unclonable.

3.2 Property Check

Now we will check these properties for a representative set of PUF constructions. The proposals we consider are basically all proposed digital intrinsic PUFs for which concrete implementation details are available, and two well studied non-intrinsic PUFs. To draw some sensible conclusions, we have to compare these PUF proposals with some non-PUF reference cases. We check against the following three reference cases which we describe in a challenge-response-like style for easy comparison with PUFs:

- A *true random number generator*. The single challenge is the request for a random number. The response is a random number extracted from a stochastical physical process.
- A very simple *RFID-like identification protocol*. The single challenge is the request for identification. The response is an identifier string which was hard-programmed in the device by the manufacturer.
- A *public key signature scheme*. A challenge is a message string. A response is signature on that message generated using a private key which was hard-programmed by the device manufacturer.

The result of this study is shown in matrix format in Table 1.

3.3 PUF-defining Properties

From Table 1 it is clear that the first four properties, i.e. evaluatable, unique, reproducible and physically unclonable, are positive ($\surd$) for all PUF proposals, while they completely distinguish them from the non-PUF reference cases. Since uniqueness is implied by physical unclonability, we could say that the set {*evaluatable, reproducible, physically unclonable*} is the least common property subset of every PUF proposal up to date, and hence can in practice be considered a definition. Being evaluatable is merely a practicality constraint and reproducibility is required to distinguish PUFs from TRNGs. The key defining property of PUFs turns out to be physical unclonability, which nicely elucidates the name *physically unclonable functions*.

Table 1. Property matrix of different PUF proposals. $\surd$ = proposal meets the property. $\times$ = proposal does not meet the property. **!** = proposal meets the property under certain conditions. **?** = it remains untested whether the proposal meets the property.

	Optical PUF [1]	Coating PUF [7]	Arbiter PUF [10] (+ variants)	Basic Ring Oscillator PUF [2]	Differential Ring Oscillator PUF [11]	SRAM PUF [14]	Latch/Butterfly PUF [18]	TRNG	Simple ID protocol	Public key signature
Evaluatable	$\surd^1$	$\surd^1$	$\surd$	$\surd$	$\surd$	$\surd^2$	$\surd$	$\surd$	$\surd$	$\surd$
Unique	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	!^{3}	!^{3}
Reproducible	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\times$	$\surd$	$\surd$
Physically Unclonable	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\times^4$	$\times^4$
Mathematically Unclonable	$\surd$	$\times^5$	$\times^6$	$\times^6$	$\times^5$	$\times^5$	$\times^5$	$\surd$	$\times^7$	$\times^7$
Unpredictable	$\surd$	$\surd$	!^{8}	!^{8}	$\surd$	$\surd$	$\surd$	$\surd^9$	$\times$	$\surd$
One-way	?	$\times^{10}$	$\times^{11}$	?	$\times^{11}$	$\times^{11}$	$\times^{11}$	$\times$	$\times$	?
Tamper Evident	$\surd$	$\surd$	?	?	?	?	?	?	$\times^{12}$	$\times^{12}$

1. Requires extra manufacturing steps and/or external measurement equipment.
2. Requires device power-up.
3. Requires explicit hard-programming of unique identifier or key.
4. Physically cloning a hard-programmed identifier or key is easy.
5. For these PUFs, a mathematical clone can be easily created by exhaustively reading out every CRP.
6. For these PUFs, a mathematical clone can be created by a model-building attack.
7. An adversary who knows the identifier/private key can easily forge a valid identification/signature.
8. These PUFs become increasingly easier to predict when an adversary learns more CRPs.
9. Unpredictability is a key requirement for a good TRNG.
10. Because these PUFs have so few challenges, a random challenge will with non-negligible probability invert a PUF response.
11. Because the output of these PUFs is basically one bit, a random challenge will with probability $\approx 50\%$ invert a PUF response.
12. If there is no additional tamper protection provided, hard-programmed identifiers and keys are not tamper evident.

4 Discussion

4.1 Unattainable Properties for *Bare PUFs*

Unpredictability is a necessary condition for many PUF applications, but it turns out that it is not always achievable for every PUF. Mathematical unclonability is even harder to obtain and up to now only the optical PUF meets this property up to some extent. However, the mathematical unclonability, and by implication the unpredictability of these *bare* PUFs can be greatly improved by turning them into *controlled PUFs*[26] (CPUFs), which is a mode of operation for a PUF in combination with other (cryptographic) primitives. A PUF is said to be controlled if it can only be accessed via an algorithm which is physically bound to the PUF in an inseparable way. Attempting to break the link between the PUF and the access algorithm should preferably lead to the destruction of the PUF. A CPUF can obfuscate the connection between its responses and the physical details of the PUF, or slow down full read-out, making mathematical cloning more difficult. It is clear that turning a PUF into a CPUF greatly increases the security, but it must be stressed that this enhanced security strongly depends on the physical linking of the PUF with the access algorithm. The exact practical and security details of this strong link are not completely clear and more research is required.

One-wayness does not seem to be a good property for bare PUFs since not one proposal was effectively shown to be one-way, and most are not. CPUFs might offer a form of one-wayness, however it will be based on the strength of its cryptographic primitives in stead of on the used PUF.

Regarding tamper evidence, which is considered a key PUF property in some works, there is much uncertainty due to a lack of experimental verification. Up to now, tamper evident characteristics were only empirically demonstrated for the (non-intrinsic) optical [1] and coating PUFs [7]. Future investigations showing either positive or negative results concerning the tamper evidence of intrinsic PUFs will be of great value.

4.2 Formalization of PUF Properties

In order to make strong claims on the security of PUFs and PUF applications, it is necessary to come up with a formalized version of the property descriptions in Sect. 3. This formalization will act as a convenient interface between the people involved in the practical implementation of a physically unclonable function and the people designing PUF-based security primitives and applications. We acknowledge that for some of the properties, coming up with a formal definition is far from trivial. Especially the more practical ones, i.e. physical unclonability and tamper evidence, will be hard to fit into a theoretical framework. Moreover, even from a practical point of view it is not yet exactly clear what these properties stand for. As already discussed, for tamper evidence further experiments on intrinsic PUFs are highly recommended in order to get a better feeling of

its feasibility. Physical unclonability, although considered to be the key property of PUFs, is for the moment a rather ad-hoc assumption primarily based on the apparent hardness of measuring and controlling random effects during manufacturing processes. However, for a number of intrinsic PUF proposals, it is not clear how realistic this assumption is. Further research into these topics is definitely required.

4.3 A Note on Mathematical Unclonability

We already stated that mathematical unclonability is unattainable for all bare intrinsic PUF proposals up to date, either due to the susceptibility to model-building attacks, or due to the small number of available CRPs which allows for a full read-out of the PUF. It is not clear whether this restriction is a sign of an underlying physical bound on the number of unpredictable CRPs which is obtainable for any intrinsic PUF, or whether this is merely a result of the particular PUF constructions which have been proposed thus far. The following open question can be stated: "Is it possible to construct an intrinsic PUF with 1) a very large (exponential?) number of CRPs, for which 2) it is practically infeasible to build and execute a model predicting unknown responses based on observed CRPs?".

5 Conclusion

Through a brief but concise overview of a representative set of PUF proposals from literature, both intrinsic and non-intrinsic, we tried to carry across the notion of which constructions we naturally identify to be PUFs, and which not. In an attempt to capture this notion in a concrete description, we establish a number of clear-cut but still informal properties and check the different constructions against them. After this study, we were able to identify the least common subset of properties which distinguishes all PUFs from a number of considered non-PUF reference cases. As it turns out, and as is nicely put forward by its naming, the key property of PUFs is physical unclonability. Additionally, this comparative study exposes some gaps and open questions in our knowledge of PUFs, both on a practical and a theoretical level. We discussed some of these topics which could lead to very interesting future investigations.

References

1. Pappu, R.S.: Physical one-way functions. PhD thesis, Massachusetts Institute of Technology (March 2001)
2. Gassend, B., Clarke, D., van Dijk, M., Devadas, S.: Silicon physical random functions. In: ACM Conference on Computer and Communications Security, New York, NY, USA, ACM Press (2002) 148–160
3. Bauder, D.: An anti-counterfeiting concept for currency systems. Technical Report PTK-11990, Sandia National Labs, Albuquerque, NM (1983)

4. Tolk, K.: Reflective particle technology for identification of critical components. Technical Report SAND-92-1676C, Sandia National Labs, Albuquerque, NM (1992)
5. Commission on Engineering and Technical Systems (CETS): Counterfeit Deterrent Features for the Next-Generation Currency Design. The National Academic Press (1993) Appendix E.
6. Armknecht, F., Maes, R., Sadeghi, A.R., Sunar, B., Tuyls, P.: Memory leakage-resilient encryption based on physically unclonable functions. In Matsui, M., ed.: Advances in Cryptology - ASIACRYPT 2009. Volume 5912 of Lecture Notes in Computer Science., Tokyo,Japan, Springer-Verlag (2009) 685–702
7. Tuyls, P., Schrijen, G.J., Škorić, B., van Geloven, J., Verhaegh, N., Wolters, R.: Read-proof hardware from protective coatings. In: Cryptographic Hardware and Embedded Systems Workshop. Volume 4249 of LNCS., Springer (October 2006) 369–383
8. Guajardo, J., Škorić, B., Tuyls, P., Kumar, S.S., Bel, T., Blom, A.H., Schrijen, G.J.: Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions. Information Systems Frontiers **11**(1) (2009) 19–41
9. Dejean, G., Kirovski, D.: Rf-dna: Radio-frequency certificates of authenticity. In: CHES '07: Proceedings of the 9th international workshop on Cryptographic Hardware and Embedded Systems, Berlin, Heidelberg, Springer-Verlag (2007) 346–363
10. Lee, J.W., Lim, D., Gassend, B., Suh, G.E., van Dijk, M., Devadas, S.: A technique to build a secret key in integrated circuits for identification and authentication application. In: Proceedings of the Symposium on VLSI Circuits. (2004) 176–159
11. Suh, G.E., Devadas, S.: Physical unclonable functions for device authentication and secret key generation. In: Design Automation Conference, New York, NY, USA, ACM Press (2007) 9–14
12. Majzoobi, M., Koushanfar, F., Potkonjak, M.: Techniques for design and implementation of secure reconfigurable pufs. ACM Trans. Reconfigurable Technol. Syst. **2**(1) (2009) 1–33
13. Rührmair, U., Sölter, J., Sehnke, F.: On the foundations of physical unclonable functions. Cryptology ePrint Archive, Report 2009/277 (2009)
14. Guajardo, J., Kumar, S.S., Schrijen, G.J., Tuyls, P.: FPGA intrinsic PUFs and their use for IP protection. In: Cryptographic Hardware and Embedded Systems Workshop. Volume 4727 of LNCS. (September 2007) 63–80
15. Holcomb, D.E., Burleson, W.P., Fu, K.: Power-up sram state as an identifying fingerprint and source of true random numbers. IEEE Trans. Comput. **58**(9) (2009) 1198–1210
16. Maes, R., Tuyls, P., Verbauwhede, I.: Intrinsic pufs from flip-flops on reconfigurable devices. In: 3rd Benelux Workshop on Information and System Security (WISSec 2008), Eindhoven,NL (2008)
17. Su, Y., Holleman, J., Otis, B.: A 1.6pj/bit 96% stable chip-id generating circuit using process variations. In: Solid-State Circuits Conference, 2007. ISSCC 2007. Digest of Technical Papers. IEEE International. (Feb. 2007) 406–611
18. Kumar, S., Guajardo, J., Maes, R., Schrijen, G.J., Tuyls, P.: Extended abstract: The butterfly PUF protecting IP on every FPGA. In: Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on. (June 2008) 67–70
19. Buchanan, J.D.R., Cowburn, R.P., Jausovec, A.V., Petit, D., Seem, P., Xiong, G., Atkinson, D., Fenton, K., Allwood, D.A., Bryan, M.T.: Forgery: 'fingerprinting' documents and packaging. Nature **436**(7050) (July 2005) 475

20. Bulens, P., Standaert, F.X., Quisquater, J.J.: How to strongly lonk data and its medium: the paper case. In: IET Information Security (to appear). (2010)
21. Hammouri, G., Dana, A., Sunar, B.: CDs Have Fingerprints Too. In: CHES '09: Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, Berlin, Heidelberg, Springer-Verlag (2009) 348–362
22. Indeck, R.S., Muller, M.W.: Method and apparatus for fingerprinting magnetic media (November 1994) US Patent No. 5365586.
23. Vrijaldenhoven, S.: Acoustical Physical Uncloneable Functions. Master's thesis, Technische Universiteit Eindhoven, the Netherlands (October 2005)
24. Lofstrom, K., Daasch, W.R., Taylor, D.: IC Identification Circuit Using Device Mismatch. In: In Proceedings of ISSCC 2000. (2000) 372–373
25. Helinski, R., Acharyya, D., Plusquellic, J.: A physical unclonable function defined using power distribution system equivalent resistance variations. In: DAC '09: Proceedings of the 46th Annual Design Automation Conference, New York, NY, USA, ACM (2009) 676–681
26. Gassend, B., Clarke, D., van Dijk, M., Devadas, S.: Controlled physical random functions. In: ACSAC '02: Proceedings of the 18th Annual Computer Security Applications Conference, Washington, DC, USA, IEEE Computer Society (2002) 149